

AFFIDAVIT OF BORDER PATROL AGENT CHAD D. EASTERDAY

Your affiant, Chad D. Easterday, Border Patrol Intelligence Agent of the United States Border Patrol, being duly sworn, does depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1) I am a Border Patrol Intelligence Agent (BPA-I) with the United States Border Patrol (USBP) assigned to the Tucson Sector Intelligence Unit. I have 23 years of total federal service and have been employed by USBP for 17 years.

2) I received law enforcement training at the Federal Law Enforcement Training Center in Artesia, New Mexico, in areas such as constitutional law, applied authority, immigration law, customs law, and smuggling methods used by criminal organizations. Throughout my career, I have received advanced training in constitutional law, investigative techniques, interviewing and interrogation techniques, plain clothes surveillance operations, and other skills needed to conduct criminal investigations. Additionally, during my career, I served as a Drug Enforcement Administration Task Force Officer.

3) During my career as a Border Patrol Agent, I have conducted criminal investigations pertaining to the detection, interdiction, and arrest of narcotics smugglers, alien smugglers, and aliens illegally present in the United States. During these investigations, I have acted as a case agent; conducted surveillance; seized narcotics; apprehended illegally smuggled non-citizens; handled evidence; submitted complaints, interviewed suspects and material witnesses; presented case development to the United States Attorney's Office; testified before a jury; drafted and served warrants.

4) Based on my training and experience I know that drug traffickers and human smugglers commonly use electronic equipment to aid them in their smuggling activities. This equipment includes, but is not limited to, smart phones, tablets, computers, video gaming systems, radios, and electronic surveillance equipment.

5) The statements contained in this affidavit are based on information provided by fellow Border Patrol Agents, criminal investigators, my observations and based on my training and experience as a Border Patrol Agent and Task Force Officer. Since this affidavit is submitted for the

limited purpose of securing a search warrant, I have not included all facts known to me regarding this investigation. I have set forth facts that establish probable cause to believe that the suspects/defendants referred to in this investigation conspired with each other and other known and unknown individuals, wherein they jointly facilitated, either verbally or electronically, the smuggling of undocumented non-citizens into the United States. This affidavit is intended to show only that there exists sufficient probable cause for the requested warrant and does not portray all my knowledge about this matter. This affidavit is intended to show only that there exists sufficient probable cause for the requested warrant and does not portray all my knowledge about this matter.

PURPOSE OF THIS AFFIDAVIT

4) I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession and the extraction from that property of electronically stored information described in Attachment B.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5) The property to be searched consists of one wireless telephone, further described as a blue Motorola smartphone bearing IMEI (355008321572517), (hereafter referred to as Target Phone), seized from Alejandro Rivera. The Target Phone is currently secured at the U.S. Border Patrol Station in Sonoita, Arizona. The Target Phone is sealed in a Department of Homeland Security Evidence Bag with a signed Form 6051S Custody Receipt for Seized Property and Evidence.

6) The requested warrant would authorize the forensic examination of the Target Phone. It would potentially identify electronically stored data to include: any telephone numbers, including but not limited to numbers called, numbers stored for speed dial, pager numbers, names and addresses, electronically stored voice and text messages, calling card numbers, text messages, photos, videos and/or identify information that may be stored in the memory of the Target Phone, for items described in Attachment A (incorporated herein by reference).

BACKGROUND ON SMARTPHONES

7) Based upon my knowledge, training, and experience, as well as information related to me by law enforcement officers and others experienced in the forensic examination of electronic communication devices, I know that certain types of cellular telephones referred to as “smartphones” (such as the Target Phone) generally offer more advanced computing ability and internet connectivity than standard cellular telephones. Provided that internet access has been purchased through an electronic communication service provider for a particular smartphone, a smartphone is capable of running complete operating system software, has full access to the internet and/or electronic mail (including file attachments), is capable of text and instant messaging, can create and edit documents created with computer software, is capable of storing large amounts of data, and can be interfaced with desktop and laptop computers.

8) As described in Attachment B hereto, this affidavit seeks permission to locate not only data files that might serve as direct evidence of the crimes described in the warrant, but also for evidence that establishes which individual(s) used the device as well as the purpose of their use. Additionally, this affidavit seeks information about the possible location of other evidence.

9) As described in Attachment B hereto, this affidavit also seeks permission to search and seize certain electronic records that might be stored within the device. Some of these electronic records might take the form of files, documents, or other data that are user generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

10) Although some of the records requested in this affidavit might be found in the form of user-generated documents (such as electronic format documents, picture, and movie files), electronic communication devices (such as the Target Phone) can contain other forms of electronic evidence that are not user-generated. In particular, an electronic communication device may contain records of how it has been used and/or the person(s) who utilized the electronic communication device. Based upon my knowledge, training, experience, as well as information related to me by law enforcement officers and other persons involved in the forensic examination of electronic communication devices, I know that:

- a. Data on electronic communication devices not currently associated with any file can provide evidence of a file that was once on the electronic communication device, but has since been deleted or edited, or of a deleted portion of a file;
- b. Virtual memory paging systems can leave traces of information on an electronic communication device that can be used to determine what tasks and processes were recently in use;
- c. Web browsers, e-mail programs, social media platforms, and chat programs store configuration information on the electronic communication devices that can reveal information such as online nicknames and passwords;
- d. Operating systems can record additional information, such as the attachment of peripheral electronic devices, and the number of occasions in which the peripheral electronic devices were accessed;
- e. Computer file systems can record information about the dates that files were created and the sequence in which they were created. This information may be evidence of a crime and/or indicate the existence and/or location of evidence in other locations on the electronic communication device;
- f. When an electronic communication device has more than one user, files can contain information indicating the dates and times that the files were created as well as the sequence in which the files were created, and whether a particular user accessed other information close in time to the file creation dates, times, and sequences;
- g. The types of evidence described above may be direct evidence of a crime, indirect evidence of a crime indicating the location of evidence or a space where evidence was once located, contextual evidence identifying an electronic communication device user, and contextual evidence excluding an electronic communication device user. All of these types of evidence may indicate ownership, knowledge, and intent to commit a given offense;
- h. The foregoing type of evidence is not “data” that can be segregated, that is, this type of information cannot be abstractly reviewed and filtered by a seizing or imaging agent and then transmitted to investigators. Rather, evidence of this type is a conclusion, based on a

review of all available facts and the application of knowledge about how electronic communication devices operate and how electronic communication devices are used. Therefore, contextual information necessary to understand the evidence to be seized, as described in Attachment B also falls within the scope of the warrant.

CHARACTERISTICS OF INDIVIDUALS INVOLVED IN HUMAN SMUGGLING
ORGANIZATIONS

11) Based upon my knowledge, experience, and training in human smuggling investigations, as well as the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common amongst individuals involved in human smuggling. Individuals involved in human smuggling activity tend to:

- a. Retain records pertaining to financial transactions and the persons for whom the transactions are being conducted;
- b. Collect data pertaining to other co-conspirators involved in human smuggling activity, including how many aliens were smuggled, as well as money owed and/or paid;
- c. Possess and maintain records reflecting bank transactions and/or money transfers;
- d. Maintain collections of records that are in a digital or electronic format in a safe, secure, and private environment, including electronic communication devices (such as the Target Phone). These records are often maintained for several years and are kept close in close proximity to the human smuggler, usually at the individual's residence, to enable the human smuggler to review the records, which are highly valued;
- e. Correspond with and/or meet with other human smuggler associates to share human smuggling information and/or materials;
- f. Retain correspondence from other human smugglers co-conspirators relating to human smuggling; and
- g. Maintain lists of names, addresses, and/or telephone numbers of individuals with whom the human smuggler has been in contact and/or conducted human smuggling activity.

12) A second telephone will often be provided to load drivers by the coordinator of the

smuggling event. The second telephone will be used during the commission of the crime to talk to scouts, and other vehicles, and parties involved. This phone will be used to track the progress of the load. Additionally, the coordinator will use the provided telephone to update the driver with information regarding any changes or destination information for the driver.

13) In my training and experience load drivers are instructed to turn off telephones while at checkpoints. This is done to prevent scouts, and other participants in criminal activity, from excessively calling the load driver and giving away information or arousing suspicion.

14) Based on the above information, the device requested to be searched may contain evidence such as: identifying serial numbers, telephone numbers, including numbers called, received, missed, and stored for speed dial, stored names, addresses, and contact telephone/direct connect numbers from the device's directories, and identifying information that may be stored in the device's memories, including any/all call logs, contact directory, stored voicemails, text messages, email messages, stored calling card numbers and digital photographs, and/or stored electronic and oral communications, and stored email/internet access information. Based on my training and experience, I know that human smugglers utilize cellular telephones and electronic devices capable of text and email messaging, as well as social media applications, to arrange, coordinate, and communicate with other criminal associates the transportation and delivery of illegal aliens. Additionally, they often use these cellular devices to relay information designed to allow the human smuggler to pass undetected through certain areas, such as Ports of Entry and Border Patrol Checkpoints. If a human smuggler does not respond, co-conspirators continue to attempt to make contact or send a series of demands for the transporter to perform when encountered by law enforcement, such as deleting any information in the phone or refraining from talking to law enforcement. These attempts will cause the phone to activate excessively following the initial encounter with law enforcement, as well as during the search of the vehicle.

///

PROBABLE CAUSE

15) On December 11, 2024, the target of an investigation identified as Alejandro Rivera, hereinafter referred to as Rivera, was arrested in a human smuggling event. Agents conducted surveillance of Rivera's smuggling event in which a Chevrolet Tracker was used to transport one undocumented migrant. During surveillance agents observed Rivera, the operator of the Chevrolet Tracker, using a cellphone while waiting at a stop light in Rio Rico, Arizona. During this observation agents observed the passenger of the vehicle who was later identified as an undocumented migrant in this smuggling event.

16) On December 11, 2024, the Chevrolet Tracker which Rivera was operating, was seized as it was used in a smuggling event. During interviews, the undocumented migrant being transported by Rivera, stated that he observed Rivera using his cellphone and could hear Rivera using code words to communicate with someone. The undocumented migrant also stated that Rivera also used a code word to describe a landmark. Based on my training and experience smugglers will often use code words as a layer of anonymity and a concealment method for their communications during illicit activity. Drivers in these events will often have a "scout" or lookout nearby in which they maintain constant communications during the smuggling event. Rivera's communications while using his cellphone during this smuggling event are indicative of coordinating with another co-conspirator for this human smuggling event. Seized from Rivera during this event is a blue Motorola smart phone bearing the IMEI of 355008321572517. During the interview with Rivera, he confirmed that it was his phone.

TECHNICAL TERMS

19) Wireless telephone: A wireless telephone (or mobile telephone or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers

in electronic “address books;” sending, receiving and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

20) Digital camera: A digital camera is a camera that records pictures and video as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos. Most cell phones currently manufactured contain digital cameras as a standard feature.

21) Portable media player. A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock or games. Most cell phones currently manufactured contain portable medial players as a standard feature.

22) Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state. Most cell phones currently manufactured allow the use of the Internet as a standard feature. Further, most current cell phones allow the user

to transmit electronic messages via standard email services or specially designed communication applications between parties.

23) Based on my training, experience, research, and from consulting the manufacturer's advertisements and product technical specifications available online for these types of cell phones, and based upon my discussions with experts, I know that the cell phones which are the subject of this search warrant application most likely has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, Internet access device, as these are generally standard features. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device; evidence of where such persons were when they possessed or used the device; evidence of who such persons were with when they possessed or used the device; evidence of persons with whom they communicated when they possessed or used the device; evidence of text, email, other electronic messaging applications and voice mail communications between the person who possessed or used the device and others; and evidence of pictures and videos taken when they possessed. Navigational coordinates may also be transmitted to and/or from these devices to determine the user's location through a GPS application.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

24) Based on my knowledge, training and experience, I know that electronic devices such as the cellular phones in this case, can store information for long periods. Similarly, things that have been viewed via or uploaded to the Internet are typically stored for some period of time on the device. Additionally, computer files or remnants of such files can be recovered even if they have been deleted. This is because when a person "deletes" the information on an electronic device, the data does not actually disappear, rather, the data remains on the storage medium until it is overwritten by new data. Forensic computer experts using forensic tools and software can often recover information similar to what has been described in this affidavit.

25) As further described in this affidavit and Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence

of the crimes described on the warrant, but also forensic evidence that establishes how the cell phones were used, where they were used, the purpose of their use, who used them and when. There is probable cause to believe that this forensic electronic evidence will be on these devices, as is more fully set forth in the factual section contained herein and because:

A. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file, including text messages, video, or photographs.

B. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

C. A person with appropriate familiarity of how an electronic device works may, after examining the forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

D. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

E. Further, in finding evidence of how a device was used, the purpose of its use, who used it, when and where, sometimes it is necessary to establish that a particular thing is not present on a storage medium, for example, the absence of the entry of a name in a contact list as evidence that the user of the cell phone did not have a relationship with the party.

CONCLUSION

26) Based on the foregoing information, there is probable cause to search Target Phone identified in Attachment A for the items set forth in Attachment B hereto. Your Affiant believes

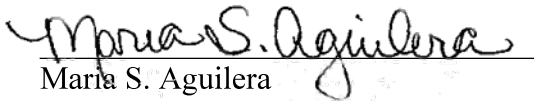
that the Target Phone contains evidence relating to the commission of a criminal offense, that is, smuggling of illegal aliens, in violation of Title 8, United States Code, Section 1324, as well as constitutes property designed for use, intended for use, or used in committing the aforementioned crime. Therefore, I request that a warrant be issued, allowing for the search of the Target Phone as described above.

CHAD D
EASTERDAY

Digitally signed by CHAD D
EASTERDAY
Date: 2025.01.09 05:58:21 -07'00'

Chad D. Easterday, Border Patrol Agent
United States Border Patrol

Subscribed electronically and sworn to
telephonically This 10th day of January, 2025.


Maria S. Aguilera
U.S. Magistrate Judge
District of Arizona

ATTACHMENT A

ITEMS TO BE SEARCHED

A blue Motorola smart phone bearing the IMEI of 355008321572517 (Target Phone). The Target Phone is currently stored at U.S. Border Patrol, Sonoita Station, Sonoita, Arizona. The Target Phone is sealed in a Department of Homeland Security Evidence Bag with a signed Form 6051S Custody Receipt for Seized Property and Evidence.

ATTACHMENT B

1. Data and/or digital files stored on or accessed through the Target Phone (as described in Attachment A) relating to violations of 8 U.S.C. § 1324, wherever it may be stored or found, specifically including:

- a. lists of contacts and related identifying information;
- b. agreements made, directions and instructions received and sent, as well as dates, places, and amounts of specific transactions;
- c. types, amounts of money obtained, received, exchanged, deposited, withdrawn, or delivered as well as dates, places, exchange rates, and amounts of specific transactions;
- d. any information related to sources of money or smuggling activity data (including names, addresses, phone numbers, or any other identifying information);
- e. all bank records, checks, credit card bills, account information, and other financial records.

2. Electronic correspondence stored on or accessed through the Target Phone relating to alien smuggling, to include emails and attached files, text messages, and instant messaging logs.

3. Information related to incoming calls, outgoing calls, missed calls, and duration of calls stored on or accessed through the Target Phone.

4. Contact lists stored on or accessed through the Target Phone, to include telephone and email contact names, telephone numbers, addresses, and email addresses.

5. Evidence of persons who used, owned, or controlled the Target Phone.

6. Logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, instant messaging logs, photographs, electronic correspondence, and telephone contact lists stored on or accessed through the Target Phone.